自治体のセキュリティポリシーとその実現に関する研究

大阪市立大学 大学院創造都市研究科
都市情報学専攻　情報基盤研究分野

井川 裕基

Study for Security Policies of Public Organization

Hiroki IKAWA

Graduate School for Creative Cities, Osaka City University

概要

自治体等の公的機関における業務の情報化・ネットワーク化が急速に進み，同時に情報資産に対する安全性の確保が不可欠となってきている．本研究では，比較的小規模な自治体における情報セキュリティ対策の状況について，その基本となる「情報セキュリティポリシー」の策定状況と実際に運用されているネットワーク環境についての調査・分析を行い，その傾向と問題点の抽出および技術的な解決策についての提案を行う．また，実環境においてより積極的にセキュリティを確保するための技術について検討をおこない，それらのひとつとして，自律型のエージェント機能について提案を行う．

1. はじめに

近年，地方自治体など公的機関の業務環境の情報化が進んでおり，従来からの徴税や住民記録の届出システムをはじめとして，多くの住民サービスや行政活動がコンピュータと庁内外のネットワーク上で行われるようになってきている．また財務や資産管理のシステムや情報交換のためのグループウェアなど，組織体としての運用のために必要なシステムも多数導入されている．

中央省庁など上位団体との間は e-Japan 戦略の成果である住民基本台帳ネットワークや総合行政ネットワーク（LGWAN）で接続され，また各省庁・部局との個別の行政システムとしてのネットワーク・端末装置が導入されるなど，多数の情報機器が日常的に使用されている．

この様な急速な ICT（情報通信技術）への依存強化の傾向は，住民サービスの向上などを理由として今後も更に進むものと考えられるが，その一方で不正侵入や情報漏洩等のリスクの増加も懸念されるため，各組織においては情報資産に対する安全性（情報セキュリティ）の確保が不可欠となってきている．

情報システムのセキュリティを確保するためには組織としてのセキュリティの方針である「情報セキュリティポリシー」を策定し，それに沿って活動する必要があるが，小規模な自治体などでは利用できる資源（職員の資質・予算など）の制限もあり，充分な態勢が整えられていないことも多いと思われる．

特に現実のシステムの設計・構築・運用では業務手順の継続性や経済的な問題などが優先される場合も多く，その運用上には各種の問題

を含んでいる.

これらの問題の解決には, もちろん組織やユーザによる取り組みが必須であるが, 技術的な面からユーザをアシストすることによりセキュリティレベルを上げる方法もあると思われる.

本研究では, 小規模な自治体を対象として「情報セキュリティポリシー」の状況と実際に運用されているネットワークシステムの事例についての調査・考察を行い, 実環境において情報セキュリティを確保する方法について検討する.

本論文では, 第 2 章において研究の方法などの概要を述べる. 第 3 章では情報セキュリティポリシーについて, その概要と国内の組織における策定状況を述べ, 自治体をはじめとするいくつかの分野における策定内容の傾向などについて比較検討する. 第 4 章では実際に自治体で運用されているネットワークを例として取り上げてセキュリティの問題について検討し, 有効と考えられる対応策についての提案を行う. 第 5 章においてはそれまでの議論を前提とし, より積極的に情報セキュリティを確保するための技術として, クライアントPC上で自律的に動作して各種のセキュリティ情報やポリシーを自動的に収集・更新し, これらを元にユーザをアシストする“セキュリティのためのエージェント機能”についての提案を行う.

2. 研究の概要

本研究の主な目的と方法を, 以下の様に設定する.

2.1 目的

比較的小規模[1] な自治体における情報セキュリティへの取り組みの状況について調査・分析を行い, その状況や取組方針の傾向を探るとともに, 現状の問題点の抽出とネットワーク技術面からの改善策を検討する. また, より積極的なセキュリティ確保のための技術についての提案を行う.

2.2 方法

組織体としての情報セキュリティに対する基本となる考え方である「情報セキュリティポリシー」について, その策定状況や内容の傾向について調査を行う.

企業・大学・自治体の各分野について, 統計情報・ポリシーの内容などを収集して比較・分析を行い, 自治体分野における傾向について考察する.

各分野における情報セキュリティポリシーの策定状況は, 総務省がアンケートなどにより定期的に調査を行っており, その結果が「報道資料」[1)] として公開されているのでこれを参照する.

ポリシーの内容については, 実際に策定されたものや策定案として検討に使用されたものを収集するほか, 業界団体などが「ガイドライン」や「サンプル」などとして公開 [2)] しているものを収集し, 検討の対象とする.

実際の現場で運用されているネットワークシステムにおける情報セキュリティに関する取り組みについて検討するため, 筆者の過去の業務経験から, 適当な規模の自治体におけるネットワークシステムの構成内容を基本とし同規模のいくつかの自治体について象徴的な部分を抽出した事例を, 対象として使用する.

3. 情報セキュリティポリシー

この章では, 研究の対象となる情報セキュリティポリシーの概要や目的, 各分野での策定状況について調査した結果について述べる.

3.1 情報セキュリティポリシーの概要

3.1.1 目的

情報セキュリティポリシーとは, 組織が情報セキュリティに関してどのように行動すべきかにつ

1 この論文では, 概ね人口 10 万人以下程度の地方自治体を想定している.

いての規約を文書化したものである. [2]

組織体としての情報セキュリティを確保するためには, 情報そのものの取り扱い方が個人の判断などに左右されることのないよう, 組織として統一された方針を持ち, 各自がそれに沿って活動を行う必要がある.

情報セキュリティポリシーは, この様な内容を明文化したものである.

ホームページ上の情報の改竄事故などを契機に, 政府は情報セキュリティポリシーの策定とそれに基づく対策を進めており地方自治体もこれに追随しているが, 厳密なポリシーの策定には大きな負担を伴うこともあり市町村などの小規模な自治体では具体的な整備が充分に進んでいるとは言い難い.

ポリシーの策定にあたっては, 自組織が保有する各種の「情報」について, それぞれの重要性などを分析し, またそれらをどのような脅威(リスク)からいかに保護すべきかを取り決め, その為に組織として何をすべきかについて「体制」「人的・物理的・技術的対策」「運用」等の内容が検討される.

3.1.2 一般的な構成内容

具体的なポリシーの例などは各分野の業界団体・所轄省庁等が公表・周知を行っている.

代表的なものに平成 12 年 7 月 18 日に内閣高度情報通信社会推進本部(IT 戦略本部)が公表している「情報セキュリティポリシーに関するガイドライン」[3] などがある. 各組織ではこのような内容を参考にした上で, 組織の目的や取り扱う情報の内容に沿って自組織に合ったポリシーを策定する.

これらのポリシーに基づき, 具体的な対策や規則, マニュアル類の整備など実環境でのセキュリティ確保の為の施策・手続きが策定される. この部分を独立に「情報セキュリティ対策」と呼ぶ場合もあるが, 本論文ではこれを含め広義の「セキュリティポリシー」という言葉を使用する.

2 本来, セキュリティとは各種の設備・人的資源・情報資源等に対する保全・安全に関する全般のための概念であるが, 本論文ではその中の「情報資源」の部分について議論を行う.

3.2 各ドメインにおける比較

情報セキュリティポリシーの実例やガイドラインを対象に, その策定内容のいくつかの部分について比較・分析を行い, 自治体におけるセキュリティに対する姿勢についての考察を行う.

3.2.1 策定の状況

各組織の目的や位置付けは所属する分野内では概ね共通するため, 情報セキュリティポリシーにも共通する部分が多く, 分野間ではそれぞれに特徴的なものであると考えるのが一般的である.

しかし実際に各分野のセキュリティポリシーを比較してみると, 中心的な項目の多くに前出の内閣 IT 戦略本部が挙げているガイドラインと共通する部分が見られる. これは政府の方針に沿うという事と共に, 各分野や組織にとっての独自のポリシーを策定することが, 労力(経済)的にも能力的にも大きな負担であることをも示すものと考えられる.

国内の各組織における情報セキュリティポリシーの策定率などは以下の様である.

- **企業分野**

  海外の企業や政府機関との契約の際に必要な国際標準の認証取得などのために早くから取り組んでいた企業もあるが, 総務省の調査報告 [4] によれば, セキュリティポリシーを策定済もしくは策定作業中であるのは, 2002 年には大企業で 49%, 中小企業では 16%であり, 2004 年 7 月の時点でも, 大企業で 56%に留まっている.

- **大学分野**

  大学等の高等教育機関でも, ネットワーク利用の普及と教育環境や事務処理などの ICT 化に伴い, セキュリティポリシーが整えられつつある[5)6)7)8)9)10)11)12)13)14)15)]. しかしその割合

は 2004 年 7 月の時点においても，策定済・作業中を合わせて約 36%と非常に低い [16].

- **自治体分野**

公的な組織では前述の様に政府の主導により情報セキュリティポリシーの策定を推進しているが，地方公共団体では総合行政ネットワーク（LGWAN）への接続のために整備を行った例が多い．

総務省の調査 [17] によれば，都道府県では 2004 年 7 月時点でセキュリティポリシーの策定率が 100%に達しているが，市区町村では同時点で 80%に留まっている．（図 1:情報セキュリティポリシーの策定状況）

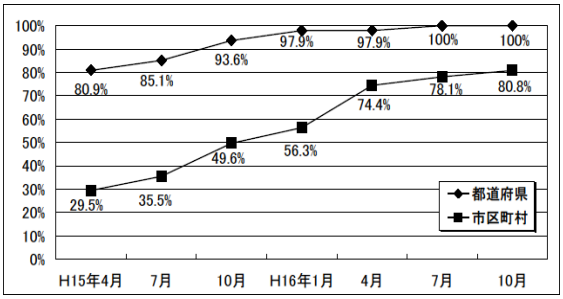

図 1:情報セキュリティポリシーの策定状況

3.2.2 情報資産の区分

組織の保持する情報資産には，どの組織にもほぼ共通のものと，組織（あるいは所属する分野）によって特徴的なものがある．それらの情報は，機密性・完全性・可用性などの視点によって分類され，その重要度によりレベル分けが行われる．

各分野による特徴が顕著となるのは最もセキュリティレベルの高い情報である．これらの情報をどの分野にも共通に挙げられているものと各分野に特有のものに分けて例示する．

- **共通のもの**

情報システム自身に関する情報（サーバ，ネットワークなど）
人事情報（評価，スタッフの個人情報など）
内部規約
各種契約関連の書類

- **企業分野に特有のもの**

顧客情報
経営関連情報（業務計画，商取引情報）
案件情報・提案書・見積書
商品情報
仕様書・設計書

- **大学等の分野に特有のもの**

学生の個人情報（基本 4 情報，成績など）
組織の運用に関連する個人情報（付属病院のカルテなど）
業績情報（蓄積された実験データなど）

- **自治体分野に特有のもの**

住民情報（基本 4 情報，印影，健保・医療など）
行政関連情報（施策案，債権者情報など）

これらの差異は基本的には組織の目的によるものであるが，分野によっては法令により保存・管理が義務付けられているものもある．

自治体分野においては主たる取り扱い情報が住民の生命や権利に直結するものである．これは，他分野の情報がどちらかというと組織自体の目的の遂行や維持のために必要な情報であるのに対して特徴的な部分となっている．

3.2.3 脅威と打撃

情報資産に対する脅威（リスク）は，主としてその流出・改竄・消失（もしくは停止）である．

脅威そのものの種類は概ねどの組織も同様であるが，リスク発生時に受ける打撃（インパクト）は，各分野によって大きく異なる．

- **企業分野**

情報の多くはリスクをこうむった際の金銭的な損害として計算できる．直接的な損害ではない場合でも，経験則などから推定することが可能な場合が多い．

- **大学等の分野**

リスク発生時のシステム停止など運用上の被害を除けば，ほとんどは信用の失墜など社会的なものである．逆にこのことが，この分野で

の情報セキュリティポリシー策定の推進を抑制している可能性もあると思われる.

・ **自治体分野**

主たる情報資産である住民情報は，流出・改竄・消失の許されないものであり，原則として金銭的な被害に置き換えられないものであるが，流出時の賠償金などの形で換算することが可能な場合もあり，リスク発生時の打撃の大きさについてもある程度推定できるようになってきていると考えられる.

また業務の情報化に伴い，大規模災害時の情報の消失や停止（利用不能）など，従来とは違った形での脅威も顕在化してきている.

3.2.4 対策

策定されたポリシーに沿って，実際の運用上の対応策が定義される. これらは「人的対策」「物理的対策」「技術的対策」などに分類して定義されるが，実際に適用されるエンドユーザの視点からはセキュリティに関する問題解決方法を「技術的なもの」「組織・規則的なもの」「個人に依存するもの」に分けて見ることができる.

ここでは各分野で策定されている内容からこれらの分類で特徴的なものを挙げる.

・ **企業分野**

技術: 業務の停止は直接損害につながる. 安定稼動に向けた対策が厳重に行なわれる

組織: 組織としての目標（収益を上げる）に沿った規定が明確に定められ対応が行われる

個人: 外注への依存度が高くなっており，それに伴うリスクへの対処が検討されている

・ **大学等の分野**

技術: 教職員と学生の区分，持込 PC の接続など，多様な利用形態への対応を含む

組織: 不正アクセス時の利用の緊急停止などシステムの管理者の権限が明示される

個人: 違反者の処分等について通報や勧告に留まるなど明確な言及を避ける傾向がある

・ **自治体分野**

技術: 保持する情報資産の特性上，改竄・消失については特に留意されている

組織: セキュリティ対策のための体制が通常の指揮系統と同様の構成である例が見られる

個人: 担当者の役割・責任と共に免責事項を明確にしている. 問題発生時の処分等についても独自の例規を用意するなどして厳正に行われる.

自治体分野では他分野に比べて各項目が比較的厳密に（形式的に）規定されている傾向が見られる. また，ポリシーの運用も記載内容に忠実であるが，明確に記載されていない内容については事象の発生時に対応が出来ない，といった傾向も見受けられる.

体制の問題を含め，こういった問題には一定の裁量権を規定するなど，策定時には想定できない問題に対して運用時に柔軟な対応が可能となる様な体制とポリシーが必要と思われる.

4. 実際に運用されているシステム

策定された情報セキュリティポリシーは，実際に組織内で使用するコンピュータネットワークシステムの設計・構築・運用に適用される.

筆者は SI ベンダとしていくつかの組織のコンピュータネットワークシステムの設計・構築・運用支援などを行ってきた. その経験の中から，比較的規模の小さな自治体に典型的な庁内システムを例として取り上げ，こういったシステムが抱えている問題について考察する.

4.1 システムの概要

例として取り上げるシステムは，実際に運用の担当に関わる，いくつかの町役場で現実に運用されているネットワークシステムに典型的なものである. 取り上げるネットワークシステムでは以下の点に留意して構築・運用されている.

システム構築には全庁的な高度情報化計画に従って以下のような目的が掲げられる.

・住民サービスの向上
・地域活性化の為の情報ネットワークの形成
・国・県の情報化推進施策への対応を考慮
・業務を情報化し事務の効率化を図る
・情報基盤の整備
・情報活用能力の向上

セキュリティ面では以下のような項目が目標として挙げられる.

・システムの信頼性と安定性の確保(安定したサービスの提供)
・取り扱う情報の性質に応じたセキュリティレベルの確保

実際の構築・運用においては以下のような点に留意される.

- **安全対策**

  技術面: 情報の分離, 不正侵入防止, 認証・利用者制限, 冗長化構成など

  設備面: 地震・火災・停電対策など

  運用面: 入退室管理・ドキュメンテーション・運用監視など

  制度面: 個人情報保護条例等の遵守・周知・徹底など

- **ユーザ教育**

  情報化担当の職員による, 利用教育や職員の情報モラル確立のための研修, その他のセミナーの実施など

- **ネットワークの構造**

  庁内で運用されるネットワークシステムについては, 個人情報などを保護する意味で以下の様に物理的に分離して運用され, 相互の通信は認められない

  ・住民情報系:
  行政サービスシステム用のネットワークであり, 住民の個人情報が取り扱われる

  ・内部情報系:
  組織運用の為のシステム用のネットワークであり, 財務管理やグループウェアなどのシステムが運用される

  内部情報系のネットワークでは, 比較的ノードの数や種類が多いため VLAN 機能などを利用して部門単位でネットワークセグメントを分割し, 通信の対象・内容などによりアクセス制限を設ける

このネットワーク上で稼動するアプリケーションシステムとしては以下の様なものがある.

- CS 型アプリケーション (CS: Client Server)
- WEB ベースアプリケーション
- インターネットアプリケーション(WEB, メールなど)

このネットワークの概要を図 2 に示す.

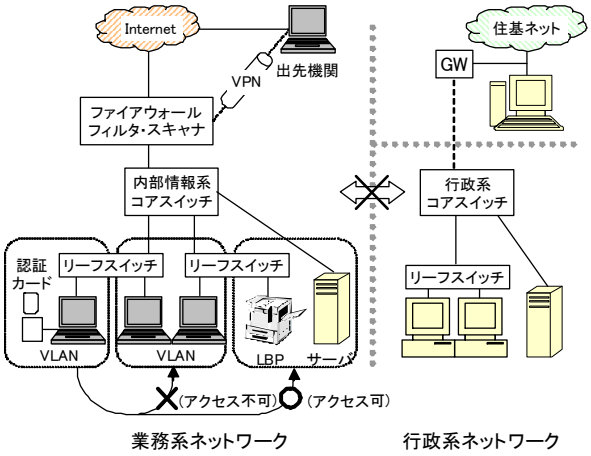

図 2 : 運用されているネットワークの概要

4.2 運用上の問題と改善策

このシステムの運用上, セキュリティ的なポイントとしては以下の様なものが考えられる.

- **トラブル等の対応**

  保守は業者の訪問により行われるが, 緊急時にはダイアルアップ回線からのアクセスによる保守も許している. トラブルの発生時はユーザから業者に通知を行う.

- **体制面での問題**
  当該の部署は庁内全体の情報化をも担当しており，議会や予算など全庁的な動向に支配されやすい．またネットワーク運用全体に関わる判断の権限は持たない．
- **グループアカウントの問題**
  運用はオフコンシステムの形態を継承する．ログオンしたままの端末を次のユーザに引き継ぐ，といった状況も日常的に見られる．
- **ネットワークの構造的問題**
  行政系・業務系に分離しているネットワークは，見かけ上は安全性が高いが，「セキュリティパッチが適切な時期に適用されない」「特定業務用の端末の台数が限定されるため使用者が替わってもログインし直さない」「別ネットワーク上のデータは記憶メディア経由で自席の PC に蓄積し加工する」といった状況も見られる．
  また，PC 等のネットワークへの接続に際しては事実上制限が設けられておらず，持ち込んだ PC の接続も容易である．

これらの問題のいくつかは，既存の技術や製品を利用することで，システムやネットワーク全体の構造を見直さずに改善が可能と思われる．

- **ユーザ個人認証の徹底**
  安全な運用には厳密な認証が必須であるが，ユーザの負担を増加させることは普及を抑制するので，手間の軽減が必要である．
- **ネットワークの管理・監視**
  ネットワークに接続されるノードは常に把握されているべきである．接続を登録制とし，また定期的な接続ノードのチェックにより，不用意な接続による問題の発生を抑制できる．
- **ネットワークの統合と制御**
  行政系と業務系のネットワークを“物理的に”分けるのではなく，VLAN や VPN によるセグメント分割とアクセス制御に置き換えることにより，使い勝手の悪さによるトラブルの誘発を軽減できる．

4.3 より高度な解決策

これらの問題に対して，技術的な対策により更に高度なセキュリティの確保が可能な点がある．特にネットワーク関連の技術は進歩が速く，新しい技術の導入が可能である．

ここでは，情報漏洩などのリスクから個人情報などを守るという視点で，最近のネットワーク技術などの面からの，解決もしくは軽減の可能性について考える．

- **業務データ流通経路の暗号化**
  ネットワークの利便性・可用性とデータの安全性を同時に確保するためには，物理的に一様なネットワークを構築し，業務システムのための通信などは暗号化され独立した論理ネットワーク上で運用する方法が適していると考えられる．暗号化には IPsec などインターネット上でも実用化され普及している技術を利用することが可能である．
- **統合認証システム**
  厳密な認証とユーザの利便性を両立するには，システムの共通の基盤としての統合化した認証システムの利用が必須である．このシステムでは，認証サーバに一度サインオンすることで，利用権限のある全てのサービスを利用するための認証を得ることができる．
- **認証つきネットワーク**
  サーバと同様，ネットワークのポート（情報コンセント）や無線 LAN の AP (Access Point) への接続の際の認証は必須となる．
  また接続時にウィルスの検疫を行うことで，可搬型の PC などを持ち込んで接続する際の安全性も確保することができる [18)]．
- **クライアント機能の限定**
  各クライアントには原則としてサービス利用以外の機能（ローカルなファイルの保存，処理の実行等）を持たせないことが望ましい．

ローカル処理が必要な PC については，動作可能なアプリケーションの限定や入出力の制限など，より厳密な管理を行うことで運用上のセキュリティを確保する．

- **認証付プリンタ**

プリンタなどの出力装置は，出力先の間違いや出力結果の取り忘れによる放置など，情報漏洩の観点では危険性が高い部分であるため，厳密な管理を行う必要がある．汎用機の時代に存在した様な，ID カードを通すことで印刷が始まるような機構は，低レベルではあるがこうした問題には有効である．

- **常態監視**

トラブルの予防や早期検出，トラブル発生時の効率的な対応などにはネットワークやサーバ等の定常的な監視と平常時の情報の保全が有効である．

但しこの作業には専門的な知識や体制が必要となるため，多くの場合庁内で行うことは難しく，アウトソーシングなどの利用の検討が必要となる．

- **ディザスタリカバリ**

障害時のデータ復旧のためにはバックアップが必須であるが，さらに大規模で広域にわたる自然災害が発生した場合などを考えると，万一失われた場合に再現の難しい情報（住民情報など）については遠隔地を含む多重の保存が望ましい．

また，現地の情報システムに深刻な被害が発生しているような場合は，緊急的に遠隔地に保存された情報を用いて一時的にサービスを行うなどの対応も検討されるべきである．

- **セキュリティのためのエージェント機能**

クライアントPC 自体が能動的にセキュリティを守る機能を持つことができれば，システム全体のセキュリティには非常に有効である．

このための方法のひとつとして，ユーザが業務に使用するアプリケーションとは別に，自律的に運用上のセキュリティを高めるためのソフトウェアをクライアント PC 上で稼動させる，ということが考えられる．

例えば顔や音声による認証によりユーザ本人が PC の前にいる時のみサービスが利用できるなどよりキメの細かな制御を行う，データの入出力やネットワークへのアクセスなどを詳細にチェックし，セキュリティ上の問題があれば注意を促す，などの機能が考えられる．

これらは一種の「エージェント機能」であり，すでに各要素の技術については概ね実用段階にあると考えられる．

このソフトウェアの動作内容については，より高度なセキュリティ確保の為の技術的な検討と共に次章で提案を行う．

これらの技術を適用したネットワークシステムの概要を図 3 に示す．

4.4 技術だけでは解決できない部分

以上の様な技術的な解決に期待できる効果は以下の様な範囲に留まる．

- セキュリティレベルの底上げ
- ミスによる事故の抑制
- ユーザ負担の低減

これらの技術的な対応だけでは完全なセキュリティの確保は難しく，特に“人”に関係する以下の様な問題は解決が困難である．

- **運用体制**

セキュリティポリシーでは CISO [3] を頂点としたセキュリティ管理組織が定義されるが，自治体の場合通常の業務の責任体制に共通した組織形態であることが多く，専門技術的な内容を含む判断や対応には適しているとは言い難い．

情報セキュリティの運用体制は，情報を取り扱う担当者を中心とし組織に対して横断的

3 Chief Information Security Officer：最高情報セキュリティ責任者

で独立した体制であることが望ましい.

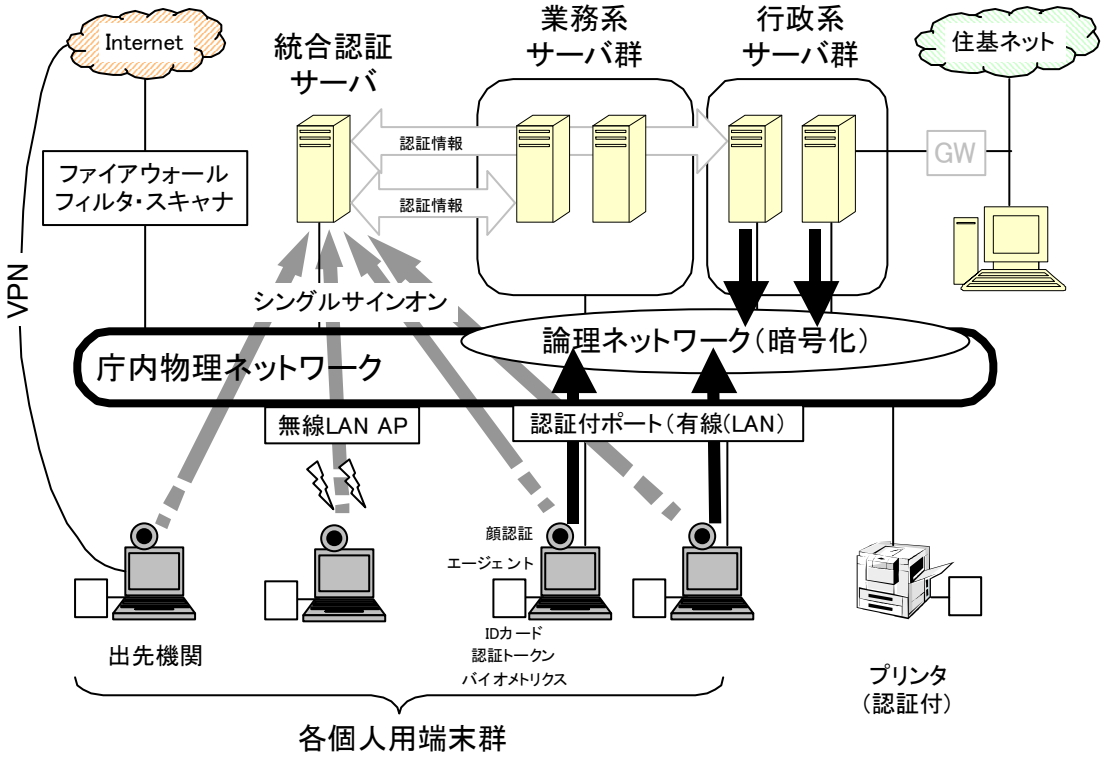

図 3:技術を適用したネットワークシステムの概要

- **管理者のスキル維持**

  運用の担当者は一定のスキルを持ち長期にわたってシステムの運用管理を担当することが望ましい. 自治体などの組織では一定の期間で職務を変わることが多く運用の技術レベルを維持することが難しいが, 安全で円滑な情報システムの継続的な運用には, 計画的な人員配置や教育などが不可欠である.

- **ユーザの意識の向上**

  最終的にはセキュリティの維持はエンドユーザの努力に依存するが, その労力はユーザにとっては負担である. 安全を確保するには根気よく教育や啓蒙活動を続けセキュリティに対する意識の向上を待つしかない.

現実的には, 完全な情報セキュリティの確保は難しい. 例えば故意による犯罪への完全な防御は不可能であるし, 大規模な自然災害には地理的な広がりを持ったシステムの冗長化が有効な対策であるが自治体のレベルでは現実的とは言い難い.

大きな脅威の発生に際しては, その被害を最小限に食い止めると同時に, 最低限の復旧内容と方法, 再発の防止, 及び被害の状況を正確に把握するための対策についての検討も重要である.

5. セキュリティのためのエージェント機能

この章では, 4 章で挙げた“セキュリティのためのエージェント機能”についての検討と提案を行う.

ここでいうエージェント機能とは, 各クライアントPC上で動作し, ネットワークを経由して自律的に最新のセキュリティポリシーなどの情報を収集

し，その内容に即してユーザの PC 利用を補助する様な機能を持ったソフトウェアである．

5.1 節では，セキュリティの確保のためにエージェント機能が有効であることを説明し，5.2 節・5.3 節では自治体の情報システム上での動作を前提としてエージェント機能の目的や備えるべき機能の概要について述べ，5.4 節では各機能の内容について詳しく検討する．

5.1 エージェント機能の有用性

4 章では実際の運用に則したセキュリティ面での改善方法と，更に高いレベルのセキュリティ確保の方法について検討したが，未知のトラブルへの回避・対応といった可能性までを考えるとネットワーク自身の機能やクライアントPC 上の静的な設定，ユーザの自発的な行動などだけでは充分な効果が得にくいと考えられる．

より高度なセキュリティの確保の為には，発生する可能性のあるトラブルを予測し抑制すること，いわゆるプロアクティブ [4] な対応が有効と考えられる．

ネットワークセキュリティ面でのプロアクティブな対応としてはファイアウォールと IDS の連携などの技術が発達してきているが，これは組織全体についてのセキュリティ，特に侵入や不正利用の抑止・ネットワークシステムの運用継続性の確保などを主な目的としているものである．

しかしながら，現実のインシデントや個人情報漏洩などの事故はクライアントPC やプリンタなど，エンドユーザがその利用現場で日常的に接する部分で発生する率が高く，しかもこの部分のセキュリティは，利用者各自の意識の問題もあって充分に確保されているとは言い難い．

こういった状況でセキュリティポリシーに則した運用をおこなう為には，クライアント PC のシステム側から積極的にユーザの操作を支援することが有効である．

また，侵入や不正利用・情報漏洩の様なトラブルが発生した場合には，状況について綿密な調査を行い，その影響の範囲をできるだけ厳密に推定することが必要となる．このためには運用中の詳細な状況についてのデータの保全が必要であるが，アプリケーションや OS のログ機能だけではなく，独自にこれらのデータを収集する機構が必要となる．

これらの観点から，エンドユーザの利用場面に近いクライアント PC 上で動作し，ユーザの操作に対する支援や詳細な利用状況などの情報収集を自律的に行うエージェント機能を提案する．

5.2 エージェント機能の要素

具体的にエージェント機能に求められる事項を検討するため，自治体の情報システムにおけるセキュリティ上の留意点を以下に挙げる．

- **住民情報など個人情報漏洩の抑止**
  （情報を預かる組織として絶対守なければならない責任）
  システムへの侵入など，不正な利用からの情報の保護
  操作上のミスや安易な運用・利用の抑制→セキュリティレベルの底上げ
- **システム運用の継続**
  （住民サービス業務の維持・遂行）
  コンピュータウィルスへの感染の防止
  DDoS 攻撃などによるシステム停止の回避
  自システムの安全性の確保
- **問題発生時の対応**
  （組織としての社会的な責任）
  発生した問題の詳細な内容の把握
  影響範囲の厳密な特定

これらの事項について，エージェント機能としてクライアント PC のシステム側からユーザの操作支援などにより実現することを考えた場合，そのエージェント機能に盛り込まれ，情報セキュリティポリシーに則って動作するべき機能として以下のような要素が考えられる．

---

4 事前予防．トラブル発生の前兆を捉え，被害が発生する前に予防的に対策すること．

- **ユーザ操作の補助（アシスト）**
  エンドユーザがクライアント PC で行う操作について，セキュリティ面での補助を行う
  このことにより手順の煩雑さやミスなどに起因するセキュリティの低下を抑制する
- **自動診断**
  自動的に自 PC や周辺の PC 相互でのセキュリティの状況を診断し，必要な対処を行う
  このことにより，ユーザの負担を軽減しながら各ノードのセキュリティのレベルを一定以上に揃えることが可能となる
- **最新のセキュリティ関連情報の収集**
  エージェント機能間，もしくは組織の情報セキュリティシステムなどと自律的に通信を行い，セキュリティ確保のために必要な情報の収集・更新を行う
- **運用情報の収集**
  ユーザの利用状況や PC の状態に関する詳細な情報（ログなど）を収集・保持する
- **チェックとトラブルの予防**
  ログやユーザの操作をチェックし，ユーザへのガイドや警告などを行う

5.3 エージェント機能の詳細

前節の内容に基づき，実際にエージェント機能で実現するべき内容の詳細について述べる．

5.3.1 ユーザ利用へのアシスト機能：認証支援

認証の手続きは，セキュリティ確保の上では非常に重要な点でありながら，これを厳密に行うほどユーザからはわずらわしく感じられるものである．特に，厳密な個人認証や離着席などに伴う状態の変更を詳細に行うことはユーザにとって大きな負担となるため，エージェント機能によるアシストが有効となる．エージェント機能は以下の様な場面においてユーザの認証の手続きへのアシストを行う．

- **サインオン**
  利用の開始時には厳密な認証を行う必要があるが，ユーザの負担を軽減するため，IC カード，顔・声などのバイオメトリクスによる認証など複数の認証手段を平行して利用し，認証サーバと通信することにより実際のユーザの負担を軽減しつつ厳密な認証を行うことができる．
- **離席・着席**
  短時間PCの前を離れる場合であっても，サインオンした状態や業務中の画面が開かれている状態は好ましくない．
  一定以上の時間ユーザがPCの前を離れた場合，これを検出して画面の暗転・ロックをするなどの処置を行う．ユーザが再度着席した時には顔認証などによりサインオン中のユーザであることを確認し，ロック状態を解除する．
- **アイドル状態の検出**
  サーバに接続している場合，長時間不必要にセッションを開いたままの状態に留める事は好ましくない．たとえユーザがＰＣの前に着席していたとしても，一定時間以上ユーザの利用がない場合は，これを検出して不要なセッションの終了などを行う．

5.3.2 ユーザ利用へのアシスト機能：ポリシーの遵守

情報セキュリティポリシーに抵触する様な操作を行おうとした場合，必要な手続き等の提示やアドバイス・警告などを行う．例えばデータファイルのメディア間コピーに際してはセキュリティポリシーの内容を提示して不用意な作業を牽制したり，ポリシーに即したデータ移動の申請手続きのガイドなどのアシストを行う．

5.3.3 自己診断・相互診断機能

自 PC についてセキュリティパッチや通信ポートの状態をチェックし，セキュリティポリシーの規定に沿って必要な処置を判断し，ユーザへの通知および（必要に応じては自動的に）対処を行う．また自 PC へ，もしくは自 PC からの通信の状態（アタックや，セキュリティの面から不適切な通信など）をチェックし，ウィルス情報等のインシデント情報との比較を行うなど，システムの健全性の診断を行い，必要があればユーザや管理者への通知・警告などを行う．

更に，エージェント機能が動作している PC 間でお互いにポートスキャンなどのセキュリティチェックを行い，問題がある場合はエージェント間で連絡を取り合ったりマスターエージェントに通知するなどの連携動作（後述）を行う．

5.3.4 連携機能

エージェント機能は，自身の動作内容を決定するために自動的にネットワーク上の各種のノードと通信を行い，情報を収集する．

- **マスターエージェント**
  各 PC 上のエージェント機能と定期的に通信することにより，全体の動作状態を把握・統括し，周辺の状況データの集約・配布を行うサーバ
- **セキュリティ情報サーバ**
  ファイアウォール・IDC などとも連携し，最新のインシデント情報やウィルス定義情報などのセキュリティ関連情報を保持しているサーバ
  各エージェント機能はこの情報を参照することでウィルス感染状況，侵入やアタックの可能性などのトレンドを知る事が出来，それに従って自システムなどの状況の確認や対応策を取ることが出来る
- **ポリシーサーバ**
  エンドユーザが遵守すべきセキュリティポリシーの情報を保持するサーバ
  エージェント機能はこの情報を元にユーザの操作を支援する
- **隣接ノード**
  各エージェント機能が直接相互に通信を行い（P2P 通信）ネットワーク上の新規ノードや不審なアクセスなどについての情報を交換する
  情報の改竄などへの耐性を高める為，通信の対象は固定せず自動的に検出することにより選択する

5.3.5 データ収集・ログ保存機能

入出力や通信内容，ネットワークトラフィックの状況，アプリケーションシステムやサーバの反応状況，ユーザのアクティビティなどについて，セキュリティ上の問題を含む可能性がない場合をも含め日常的に極力詳細な情報を収集し，ログとして保存する．

このことは，情報漏洩などのトラブルが発生した場合に，対象となる情報や漏洩の経路・範囲などの特定に必要となる情報を提供し，トラブル対処の迅速化・効率化につながるものである．

5.3.6 警告・通報機能

ログは，保存に平行して常にその内容がチェックされ，必要に応じて警告・通報などが行われる．

このことはシステムの状態の把握に有効であり，故障やトラブルによるサービスの停止の予防につながる．

警告や通報は，クライアント PC の使用者（エンドユーザ）とシステム管理者に対してそれぞれ行われる．

各機能および各種のノードとの連携の様子を図4に示す．

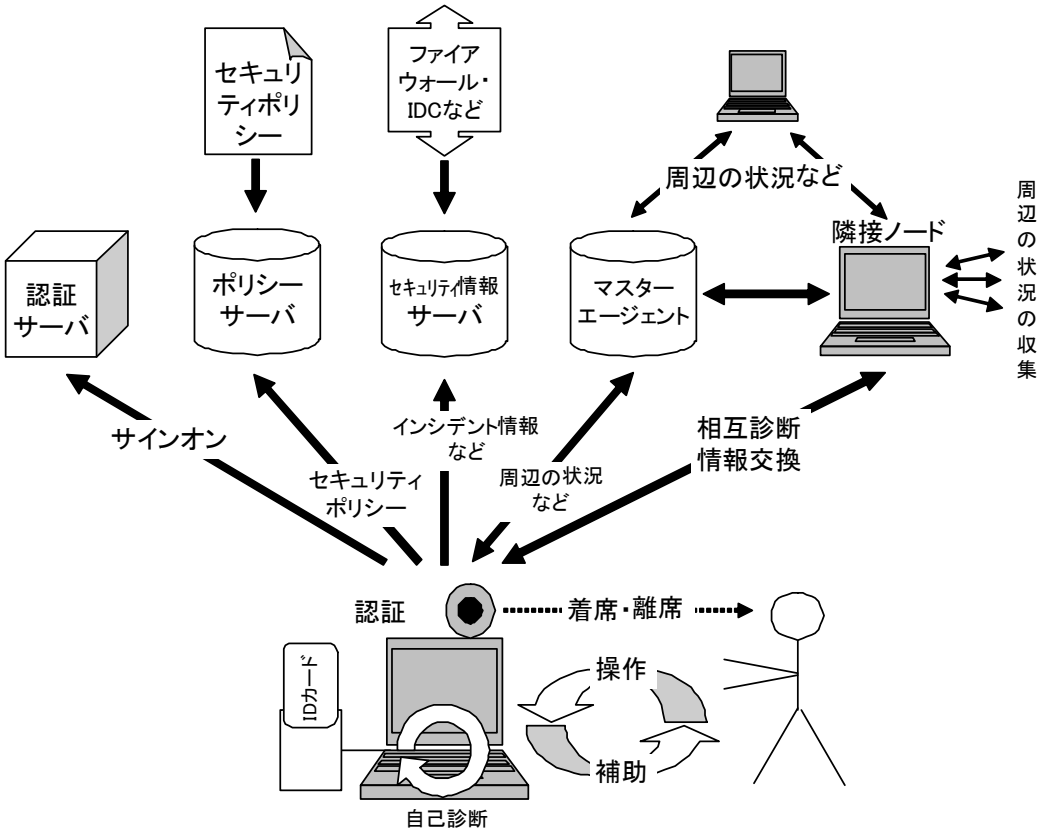

図 4:エージェントの機能と連携

6. まとめ

本論文では，比較的小規模な自治体の情報ネットワークシステムにおけるセキュリティの確保の方法を探るため，現状での情報セキュリティへの取り組みを，情報セキュリティポリシーの策定の状況と，実際の業務経験を元にした情報ネットワークシステム運用の状況から分析・検討し，その結果から現状の問題点の抽出とネットワーク技術面からの改善策を検討した．また，より高度なセキュリティ確保のための技術として，エージェント機能について提案を行った．

地方自治体，特に小規模な団体における業務のICT化は今後もますます進むものと考えられるが，それに合わせて運用の安定性への要求や漏洩などのリスクも増大し，その対応は各組織にとって大きな負担である．

このような状況を支援するような技術やサービス，枠組みなどの利用も可能になりつつあり，それらをシステムに取り込むことでより安全にシステムを運用できると考えられる．

大掛かりな施設・設備と高度な技術を持つスタッフによる運用はもちろん高いセキュリティの確保に対して有効であるが，現実に発生するトラブルの内容からはむしろ実際の運用の現場，特にエンドユーザの周辺におけるセキュリティ対策が重要であることがうかがえる．

最近では汎用のOSのセキュリティ機能も高度化しつつあるが，それだけでは自治体業務に充分なセキュリティのレベルを提供するにはまだまだ不充分であると考えられる．

組織の状況に応じた情報セキュリティポリシーの適切な策定内容と，本論文で提案を行ったエージェント機能の様な仕組みによる操作支援

の機能が，より安全な利用環境を自治体のエンドユーザ，ひいては業務の対象である住民に提供できるものと考えられる．

参考文献

1) 総務省: 報道資料, http://www.soumu.go.jp/s-news/, Jan 29 2005
2) 日本ネットワークセキュリティ協会: 情報セキュリティポリシー・サンプル 0.92a 版, http://www.jnsa.org/policy/guidance/index.html, Nov 6 2004
3) 首相官邸: 情報セキュリティポリシーに関するガイドライン, http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html, Nov 6 2004
4) 総務省: 情報セキュリティに関する実態調査結果の公表, http://www.soumu.go.jp/s-news/2004/040705_2.html, Nov 6 2004
5) 京都大学: 大学における情報セキュリティポリシーの考え方, http://www.kudpc.kyoto-u.ac.jp/Security/tosin2001.html, Nov 6 2004
6) 名古屋大学: 名古屋大学情報セキュリティポリシー, http://www2.itc.nagoya-u.ac.jp/security-policy/guideline/policy.html, Jan 29 2005
7) 兵庫教育大学:国立大学法人兵庫教育大学情報セキュリティポリシー, http://www.info.hyogo-u.ac.jp/info/hunetguide/kihon.html, Jan 29 2005
8) 京都工芸繊維大学: 京都工芸繊維大学・情報セキュリティ基本方針, http://www.kit.ac.jp/quick/security_policy.htm, Jan 29 2005
9) 三重大学: 三重大学情報セキュリティポリシー, http://www.cc.mie-u.ac.jp/cc/policy/, Jan 29 2005
10) 秋田大学工学資源学部: 国立大学法人秋田大学情報セキュリティポリシーの運用に伴って「秋田大学工学資源学部の構成員が行うこと」, http://www.str.ce.akita-u.ac.jp/~gotou/sekyu/unyou/unyou04.html, Jan 29 2005
11) 早稲田大学: 早稲田大学 情報セキュリティポリシー, http://www.waseda.jp/mnc/RULES/Security_Policy.html, Jan 29 2005
12) 関西学院: 情報セキュリティ基本ポリシー, http://www.is.kwansei.ac.jp/policy/basic.html, Jan 29 2005
13) 日本福祉大学: 日本福祉大学 情報セキュリティの基本ポリシー, http://www.n-fukushi.ac.jp/news/jyunsyu11.htm, Jan 29 2005
14) 上越教育大学: 国立大学法人上越教育大学情報セキュリティポリシー, http://www.juen.ac.jp/contents/info/porisi/0521housin.pdf, Jan 29 2005
15) 大学評価・学位授与機構: 情報セキュリティポリシー, http://www.niad.ac.jp/sub_data/securitypolicy.html, Jan 29 2005
16) 総務省: 情報セキュリティに関する実態調査結果の公表, http://www.soumu.go.jp/s-news/2004/040705_2.html, Nov 6 2004
17) 総務省: 地方公共団体における情報セキュリティポリシー（情報セキュリティ対策に関する基本 方針）等の策定状況（平成 16 年 10 月 1 日現在）, http://www.soumu.go.jp/s-news/2004/041203_2.html, Jan 29 2005/01/29
18) 三輪, 大野:「持ち込み PC 検疫機構の設計と実装」, コンピュータセキュリティシンポジウム 2004 論文集, p697
*) 井川, 中野, 大西:「セキュリティポリシーに基づいた公的組織のシステム運用への提案について」,コンピュータセキュリティシンポジウム 2004 論文集, p787